ABSTRACT OF THE DISCLOSURE

A method and an apparatus capable of realizing at a high speed an elliptic curve cryptography in a finite field of characteristic 2, in which the elliptic curve is given by $y^2 + xy = x^3 + ax^2 + b$ ($b \neq 0$) and an elliptic curve cryptography method which can protect private key information against leaking from deviation information of processing time to thereby defend a cipher text against a timing attack and a differential power analysis attack are provided. To this end, an arithmetic process for executing scalar multiplication arithmetic d(x, y) a constant number of times per bit of the private key d is adopted. Further, for the scalar multiplication d(x, y), a random number k is generated upon transformation of the affine coordinates (x, y) to the projective coordinates for thereby effectuating the transformation $(x, y) \rightarrow [kx, ky, k]$ or alternatively $(x, y) \rightarrow [k^2x, k^3y, k]$. Thus, object for the arithmetic is varied by the random number (k).